POLÍTICAS DE SEGURIDAD Y USO DEL CORREO ELECTRONICO INSTITUCIONAL DE CARABINEROS DE CHILE

a). - NORMATIVA:

- LEY 19.628, SOBRE PROTECCION DE DATOS DE CARACTER PERSONAL.
- LEY 19.223, TIPIFICA FIGURAS PENALES RELATIVAS A LA INFORMATICA.
- DECRETO NRO. 83, NORMA TECNICA PARA LOS ORGANOS DE LA ADMINISTRACION DEL ESTADO SOBRE SEGURIDAD Y CONFIDENCIALIDAD DE LOS DOCUMENTOS ELECTRONICOS.
- NCH-ISO 27001/2013 – NORMA CHILENA PARA LAS TECNOLOGIAS DE LA INFORMACION, TECNICAS DE SEGURIDAD, SITEMAS DE GESTION DE LA SEGURIDAD DE LA INFORMACION Y REQUISITOS.

b). - ALCANCE Y ACEPTACION: Esta política se aplicará al servicio de correo electrónico Institucional de Carabineros de Chile, que se ofrece desde la plataforma ICEWARP, la cual debe ser cumplida por todos los Funcionarios de la Institución, desde ahora "usuarios", los cuales aceptan sus términos y procedimientos relacionados.

c). - OBJETIVO: Ofrecer a los usuarios, una guía sobre los requerimientos mínimos que se deben cumplir, respecto del uso del correo electrónico Institucional, que se provee, como también las implicancias del mal uso. Evitar la congestión en la red de datos, provocando ralentizar el servicio y evitar problemas administrativos y/o jurídicos, debido al incorrecto uso de los recursos.

d). - RESPONSABILIDADES:

- OF. DE VIDEOCONFERENCIA Y WEBMAIL: Dependiente del Área Gestión de Servicios, del Departamento Tecnologías de la Información y las Comunicaciones L.7., su función es administrar y mantener la seguridad, disponibilidad e integridad de la plataforma de correo electrónico Institucional, dar soporte a los usuarios e informar sobre nuevas amenazas y cuidados con respecto al resguardo de la comunicación.

- USUARIOS: Todos los usuarios que mantengan habilitada una cuenta de correo bajo el dominio "@carabineros.cl", deberán cumplir lo establecido en esta política de seguridad y uso del correo electrónico Institucional, serán los responsables de su contraseña de acceso y del tratamiento de la información que en su cuenta se almacene.

e). - SOLICITUD DE HABILITACION: Para disponer de una cuenta personal alojada en la plataforma ICEWARP, el usuario deberá estar dado de alta en la base de datos del Departamento de Registro y Análisis de Información de Personal P.7., luego deberá enviar el formulario de solicitud existente en la web del Portal Institucional, en donde deberá consignar una dirección de correo electrónico valida, personal y funcional, además de aceptar los términos y condiciones estampados en esta política de seguridad y uso del correo electrónico Institucional.

La solicitud de una cuenta corporativa debe ser realizada por las Altas Reparticiones, Reparticiones, Unidades y Servicios Especializados, mediante documentación electrónica al Dpto. T.I.C. L.7., para lo cual se requiere informar el responsable de la misma, quien será la persona de contacto con el equipo de administración de correo y el nombre tentativo de la cuenta a crear.

f). - ESTRUCTURA DE LA DIRECCION DE CORREO INSTITUCIONAL: El formato de una cuenta de correo electrónico, para los alias del dominio "@carabineros.cl", es "alias_del_usuario"@carabineros.cl". El "alias del usuario" estará formado por el primer nombre seguido por un punto y el primer apellido, si el alias ya está en uso luego del primer apellido, inmediatamente se agrega la primera letra del segundo apellido, y si aun así el alias esta en uso, se irán sumando las letras del segundo apellido sucesivamente, hasta lograr el alias, o podrá utilizarse una combinación dispuesta por esta oficina de correo.

g). - ACCESO: Cada usuario tendrá acceso a la plataforma del correo electrónico Institucional utilizando su código de funcionario y contraseña, la cual será la misma para el Portal Institucional y para todos los demás portales, aplicativos o dispositivos que requieran clave de "Intranet".

h). - TIPOS DE CUENTAS:

- CUENTAS PERSONALES: Son las direcciones de correo electrónico de un usuario.

- CUENTAS CORPORATIVAS: Las cuentas Corporativas están orientadas fundamentalmente a Altas Reparticiones, Reparticiones, Unidades, Destacamentos y Servicios Especializados en general. Otros estamentos Institucionales la pueden solicitar y dicha solicitud será evaluada por Área Gestión de Servicios del Departamento Tecnologías de la Información y las Comunicaciones.

Mencionadas cuentas pueden ser utilizadas por una o varias personas conjuntamente y son gestionadas por un responsable. Por consiguiente, este tipo de cuentas no están asociadas a cargos o personas.

i). - VIGENCIA, DESHABILITACION Y ELIMINACION DE CUENTAS DE CORREO

- Vigencia: Cada cuenta de correo electrónico Institucional estará vigente mientras el usuario permanezca en las filas de la Institución. Las cuentas corporativas se encontrarán vigentes mientras exista la necesidad de su uso.

- Deshabilitación: La deshabilitación ocurre una vez que el usuario ha dejado de pertenecer a la Institución, es un proceso automatizado entre la base de datos de personal del Departamento P.7., y el servidor de correo Institucional.

- Eliminación: La plataforma de correo electrónico está sujeta a las normas establecidas en el Reglamento de Documentación Nro. 22 y es considerado como documentos varios, por cuanto su duración es de dos años, luego de ese plazo las cuentas pueden ser eliminadas.

j). - TAMAÑO DE LOS BUZONES DE CORREO

El usuario que utilice el correo electrónico institucional, podrá enviar y recibir mensajes con un tamaño de hasta 25 MB y tendrá una capacidad de almacenamiento de 200 MB. Sin perjuicio de lo anterior estas capacidades podrán modificarse de acuerdo a las necesidades y funciones de cada usuario y/o cuenta corporativa, lo que será evaluado por el Área Gestión de Servicios a petición del requirente vía documentación electrónica.

Se ha de considerar que, el correo electrónico enviado, circula por distintos servidores de Internet y que éstos imponen libremente restricciones sobre los tamaños admitidos, por lo que cuanto más grande sea el tamaño del mensaje de correo, mayor es la probabilidad de que sea rechazado, impidiendo de este modo que llegue a su destino.

k). - SEGURIDAD

Son múltiples los problemas de seguridad que pueden afectar al correo electrónico, entre los que cabe destacar:

- Robo de identidad y credenciales de acceso.
- Virus que afectan al computador.
- Worms (virus gusano) que utilizan técnicas de spam para propagarse después de infectar un computador.
- Malware y Correo no deseado (spam), etc.

Por lo anterior, se debe tener presente que, el usuario, es responsable del mantenimiento de la seguridad, tanto de su propia información, como de su cuenta asignada y contraseña. Esta no debe ser cedida o facilitada a terceros, siendo responsabilidad del propio usuario su custodia. El cambio de la contraseña debe ser periódico, con la finalidad de mantener segura sus credenciales. Los usuarios son responsables también por el tráfico y el contenido de la información de las cuentas asignadas.

l). - NORMAS SOBRE EL USO CORRECTO DEL CORREO ELECTRONICO INSTITUCIONAL:

- El correo electrónico provee de una comunicación rápida y eficiente tanto dentro como fuera de la Institución, es una herramienta de trabajo para que el personal pueda desempeñar sus labores, no siendo el medio de comunicación oficial de carabineros de chile.
- Está prohibido el uso del correo electrónico institucional para propósitos personales.
- Toda casilla de correo electrónico Institucional, está directamente vinculada al usuario, y este, es responsable del contenido y de los archivos adjuntos a cada mensaje.
- El resguardo de las claves de acceso al correo electrónico, es de exclusiva responsabilidad del usuario. Queda estrictamente prohibido divulgar, compartir ni anotar en lugares visibles y/o de fácil acceso.
- Se prohíbe el envió, mediante correo electrónico institucional, de ofertas de compra o venta. Así como también cualquier tipo de cartas en cadena, pirámides o phishing, o enviar un correo electrónico solicitando donaciones caritativas, peticiones o cualquier material relacionado.
- Se prohíbe el envío de mensajes que comprometan el prestigio o nombre de la Institución o de alguno de sus miembros.
- El envío masivo de correos se gestionará a través de la oficina de videoconferencia y webmail y/o mesa de ayuda del dpto. T.I.C., con un mínimo de 48 horas de antelación, estos mensajes de difusión no deben considerarse como spam.
- Se aconseja que si un usuario se ausenta de sus labores por un tiempo considerable (vacaciones o licencia médica), debe dejar su correo electrónico institucional con respuesta automática, donde comunique que estará ausente por un periodo de tiempo específico, indicando según sea el caso, quien lo reemplazará en el cargo que ocupa.
- Se prohíbe el intento de obtener acceso a los mensajes de correo electrónico de otro usuario.
- Se prohíbe utilizar la cuenta de correo electrónico para emitir opiniones personales en foros de redes sociales, debido que esto puede ser entendido como la declaración oficial de Carabineros de Chile.
- No se deben instalar o ejecutar archivos adjuntos que sean desconocidos. Como así mismo, no se deben enviar archivos con extensión: “.zip”, “.exe”, “.bin”, entre otros.

m). - MECANISMO DE CONTROL QUE PUEDE AFECTAR LA PRIVACIDAD:

Se podrá acceder al contenido de alguna cuenta de correo electrónico Institucional en el marco de una investigación y previa Orden Judicial.

n). - ANTISPAM Y ANTIVIRUS

La plataforma ICEWARP, dispone de diferentes sistemas encargados de filtrar y rechazar el correo electrónico considerado spam, basado en listas de reputación de los servidores que envían correos. Si un correo de origen externo se cataloga como SPAM, se marca la cabecera (el Asunto o Subject) con la etiqueta [POSIBLE SPAM].

Asimismo, la plataforma ICEWARP, analiza todo el tráfico de correo entrante y saliente, y rechaza el envío de mensajes que puedan contener virus. Cuando un mensaje es rechazado se envía una notificación al destinatario, salvo en el caso de que el virus falsifique la cabecera de origen.

o). - POLÍTICA DE LOGS

La plataforma ICEWARP mantiene por un periodo de 30 días las trazas del tránsito de correos que gestiona, guardando un archivo LOG en el servidor. Dichos LOG contiene los siguientes datos: IP de origen, remitente, destinatario fecha y hora y, si es pertinente, (salvo que se eliminase el correo por listas negras) el servidor de destino que ha procesado el correo.

p). - CONTROL DE TRAFICO, PREVENCION DE INTRUSION Y BLOQUEO DE CUENTAS

CONTROL DE TRAFICO: Nuestro servidor Barracuda, monitorea constantemente el tráfico de correo, bloqueando automáticamente la salida de correos que considere como spam o que excedan un numero de envíos determinados en un lapso de tiempo establecido.

PREVENCION DE INTRUSIONES: Serán bloqueadas automáticamente, las Direcciones IP por 60 días si se excede las 25 conexiones por minuto, por exceder 5 intentos fallidos de inicio de sesión, por exceder el número de entrega a usuarios desconocidos, falla en generar 5 veces un relay, por exceder 5 veces el reset de sesión y el envió de correos electrónicos con más de 50 MB.

BLOQUEO DE CUENTAS: Las cuentas pueden ser bloqueadas conforme a los informes de seguridad de Barracuda o según la configuración de Prevención de Intrusión. No obstante, al ser regularizadas las cuentas por los usuarios estas pueden ser desbloqueadas.

q). - ATENCIÓN DE USUARIOS, CONTACTO E INFORMACIÓN

Para consultas o dudas sobre la plataforma de correo electrónico Institucional, se debe tomar contacto en primera instancia, con la Mesa de Ayuda T.I.C., Anexo IP 22300, quienes evaluaran el requerimiento para dar solución, o lo derivaran al nivel 2, de la Oficina de Videoconferencia y Correo.

r). - BUENAS PRACTICAS PARA EL ENVIO DE CORREOS ELECTRONICOS:

1. Incluya un "Asunto" (Subject) en el mensaje. Indique en dicho campo una breve frase descriptiva del mismo. Esto facilita la lectura, clasificación y posterior recuperación al destinatario y constituye una norma de cortesía.
2. Utilice las mayúsculas y minúsculas correctamente. No se debe escribir todo el texto del mensaje en mayúsculas. Revise cuidadosamente la ortografía y redacción del mensaje. Si desea enfatizar un término, puede usar comillas, negrita, otros colores, etc. Si estima que la letra es muy pequeña, puede agrandar la letra hasta un tamaño que resulte más conveniente, pero no extravagante. El uso de mayúsculas en Internet sugiere emociones fuertes.
3. No utilice estilos con fondos de mensaje ya que aumentan el tamaño del mismo y pueden provocar problemas de recepción en el destinatario (filtrado por el sistema antivirus-antispam).
4. Debe tener cuidado con el tamaño de los mensajes. Incluir documentos de gran tamaño, imágenes o programas puede hacer su mensaje tan pesado que tenga problemas de recepción, así como un consumo de recursos innecesarios al receptor del mensaje. Cuando envíe un adjunto se debe indicar en el mensaje cuál es su contenido y su propósito para evitar que el destinatario sospeche que se trata de un virus.
5. Sea sintético. Las personas están sometidas a muchos estímulos informativos. Si su texto es muy largo, es probable que no lo lean o lo abandonen a medio camino. Las firmas automáticas deben ser lo más esquemáticas posible, tratando de evitar imágenes o información innecesaria.
6. No facilite datos personales o financieros a personas desconocidas.
7. No se debe responder al correo no solicitado (spam). Responder al correo comercial no solicitado es una forma de aumentar la cantidad de correo basura.
8. No sobrevalore la herramienta. Es probable que la respuesta a su envío sea más baja que sus expectativas. Usted puede considerar que es el medio más eficiente ya que llega directo a la casilla de sus receptores; sin embargo, éstos no siempre leen lo enviado
9. Debe evitarse el participar en el reenvío de correo no solicitado (cadenas de mensajes, rumores, publicidad, etc.).
10. Se debe respetar la privacidad de los mensajes y del destinatario. No reenvíe mensajes destinados a usted sin el permiso del remitente, sobre todo aquellos con contenido delicado o confidencial.
11. No debe abusarse de funcionalidades como el "aviso de lectura", su eficacia es escasa cuando lo utilizamos de manera indiscriminada o continuada, llegando a molestar al remitente. Se debe activar sólo en los casos en los que realmente sea necesario.
12. Es un hecho de que los buzones la cuenta de los usuarios llegan a su cuota máxima, con material que en realidad no les interesa ni han solicitado, impidiendo que reciban más correos, que sí son de su interés. Por lo anterior, se recomienda eliminar los correos innecesarios o respaldar la información en otra cuenta.

s). - REVISION DE POLITICA: Esta política de seguridad será revisada cada dos años y se procederá a la publicación de las modificaciones.

t). - SANCIONES APLICABLES: La inobservancia a la presente política de uso, quedara supeditada a las Leyes de la Republica, Reglamentos y Normas Institucionales.

PREGUNTAS FRECUENTES - FAQ's:

1.- ¿Pueden publicar mi dirección de correo electrónico Institucional en la página web de Carabineros, sin mi consentimiento?

R: Sí, con fines estrictamente profesionales y solo en casos que resulte necesario, de acuerdo con las funciones que tenga cada usuario.

2.- ¿Puedo utilizar el correo electrónico Institucional con fines personales?

R: No, debido a que el correo electrónico Institucional externamente puede ser entendido como un medio de comunicación oficial de Carabineros de Chile.

3.- ¿Puede el mando acceder a mi cuenta de correo Institucional?

R: No, sólo el Jefe de Área Gestión de Servicios y/o personal de la Oficina de Videoconferencia y Correo puede acceder al contenido de alguna cuenta de correo electrónico, en el marco de una investigación y previa instrucción Judicial.

4.- ¿Puedo facilitar mi cuenta y contraseña de correo a otro usuario de mi confianza?

R: No, las cuentas son personales y la contraseña de acceso no debe ser facilitada a persona alguna, ni quedar grabada en navegadores de internet (Internet Explorer, Google Chrome, Firefox, Opera, etc.).

5.- ¿Puedo acceder a mi cuenta de correo Institucional desde Internet, mi celular o mi conexión de internet de mi hogar?

R: Si, el acceso al portal web del correo Institucional es posible desde la red de internet y cuenta con un certificado de seguridad digital, lo que significa que es una conexión segura y el envió de credenciales por la red es cifrada. La url es https://webmail.carabineros.cl, la cual debe ser digitada en cualquier navegador de internet.

6.- ¿Puedo solicitar que dejen de enviarme correos informativos?

R: El envió de información Institucional es para el conocimiento y beneficio de los usuarios, por cuanto no es considerado como spam.

7.- He olvidado mi nombre de usuario y contraseña.

R: Su nombre de usuario siempre será su código de funcionado, con excepción de casos especiales, si ha olvidado su contraseña de acceso, consulte el manual de recuperación de contraseña existente el portal del webmail.

8.- ¿Puedo recibir virus o correo basura (spam) en mi cuenta de correo?

R: Si, sin embargo, nuestra red está siendo constantemente monitoreada pero aun así es posible que en su cuenta de correo reciba mensajes solicitando sus credenciales (nombre de usuario y contraseña), en este caso no lo debe responder, ni descargar algún archivo adjunto, solo limítese a reenviarnos ese mensaje a administrador@carabineros.cl, para proceder al bloqueo del remitente.

9.- ¿Puedo sincronizar mi cuenta de correo institucional en mi equipo celular?

R: Si, solo hay que seguir los manuales de configuración, los cuales se encuentran alojados en el siguiente **LINK.** Tanto para usuarios de Android e iOS.